JOURNAL OF NUMBER THEORY 32, 263–280 (1989)

The Delta-Lambda Configurations in Tiling the Square

ANDREW BREMNER

Department of Mathematics, Arizona State University, Tempe, Arizona 85282

AND

RICHARD K. GUY

Department of Mathematics, The University of Calgary, Calgary, Alberta, Canada T2N 1N4

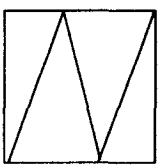
Communicated by H. Zassenhaus

Received December 31, 1986; revised July 1, 1988

1

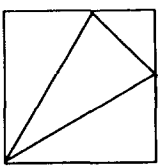
A recent study [4] has considered the problem of tiling an integer sided square with integer sided triangles. This is clearly equivalent to the problem of tiling the unit square with rational sided ("rational") triangles. A dissection into two such triangles is trivially impossible, and it is shown in [4] that a dissection into three triangles with rational sides is also impossible.

Accordingly the first interesting case is a dissection into four rational triangles. There are essentially just four possible configurations for the dissections, shown in Figs. 1–4. These configurations are referred to respectively as the nu-configuration, the delta-configuration, the chi-configuration, and the kappa-configuration. Common to the chi- and kappa-configurations is the lambda-configuration of Fig. 5. The delta- and lambda-configurations possess a duality, as indicated in Figs. 6 and 7, and



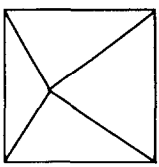
ν

FIGURE 1



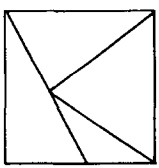
Δ

FIGURE 2



χ

FIGURE 3



κ

FIGURE 4

0022-314X/89 $3.00

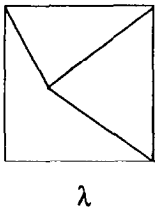


FIGURE 5

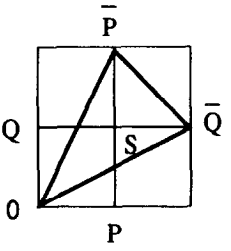


FIGURE 6

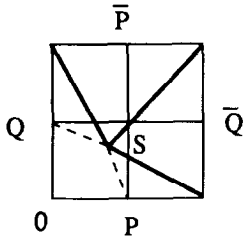


FIGURE 7

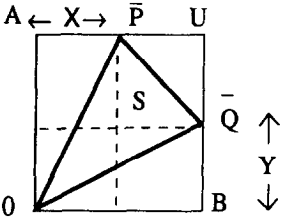


FIGURE 8

it is not difficult to show that the triangles of Fig. 6 are rational if and only if the triangles of Fig. 7 are rational.

The purpose of this note is to discuss the delta-configurations, or equivalently, the lambda-configurations. Let Fig. 8 denote a dissection into rational triangles. With OA, OB as coordinate axes, let U be the point $(1, 1)$ and S the point (X, Y), X, Y rational. It follows immediately that

$$X^2 + 1 = \text{square}$$

$$Y^2 + 1 = \text{square}.$$

Further,

$$(1 - X)^2 + (1 - Y)^2 = (\bar{P}\bar{Q})^2$$

so that

$$M = \frac{1 - Y}{1 - X}$$

satisfies

$$M^2 + 1 = \text{square}.$$

We shall call a rational number x which satisfies

$$x^2 + 1 = \text{square}$$

a rectangular number.

It is clear now that delta-configurations are characterized by solutions of the equation

$$1 - Y = M(1 - X), \tag{1}$$

where M, X, Y represent rectangular numbers.

A small computer search reveals a multitude of solutions to (1), and in the following sections we investigate this equation more carefully. We produce infinitely many parametrized solutions, and in the case of a predetermined value of M, show how to compute all solutions for X, Y. In conclusion, a numerical table of solutions is presented.

2

In (1), there is no loss of generality in putting

$$M = \frac{m^2 - n^2}{2mn}, \qquad X = \frac{r^2 - s^2}{2rs}, \qquad Y = \frac{u^2 - v^2}{2uv} \tag{2}$$

so that we seek integer solutions m, n, r, s, t, u to the equation

$$2mnrs(u^2 - 2uv - v^2) = uv(m^2 - n^2)(r^2 - 2rs - s^2). \tag{3}$$

The equation (3) is of degree 6, apparently in five-dimensional projective space. However, the very nature of the substitution (2) has ensured that (3) is homogeneous of degree 2 in each pair of variables (m, n), (r, s), (u, v). Accordingly, the geometrical interpretation of (3) is as an equation in affine three-dimensional space with coordinates m/n, r/s, u/v. As such, it is a surface.

It seems an unlikely hope that there is any straightforward description of all the rational points on this surface. We instead adopt the following approach. The surface is fibred by pencils of elliptic curves, in particular those obtained by regarding the ratio m/n as predetermined. This corresponds to predetermining the rectangular number M, that is, the slope of the line SU in Fig. 8. From a knowledge of the rational points on these elliptic curves, we recover the corresponding delta-configurations, and we shall refer therefore to solutions of a certain slope M.

3

With $r/s = R$, $u/v = U$, then (3) takes the form

$$\frac{2mn}{m^2-n^2} R[U^2-2U-1] = U[R^2-2R-1]$$

so that as a quadratic in U,

$$\left(\frac{2mn}{m^2-n^2} R\right) U^2 + \left(-R^2 + \frac{2(m^2-2mn-n^2)}{m^2-n^2} R + 1\right) U$$
$$- \frac{2mn}{m^2-n^2} R = 0.$$

The condition that the discriminant be a perfect square α^2 is that

$$R^4 - 4\frac{(m^2-2mn-n^2)}{m^2-n^2} R^3 + 2\left(\frac{m^2-4mn-n^2}{m^2-n^2}\right)^2 R^2$$
$$+ 4\left(\frac{m^2-2mn-n^2}{m^2-n^2}\right) R + 1 = \alpha^2.$$

There is now a standard transformation from an equation of this type to the more standard form of equation taken by an elliptic curve (see, for example, Mordell [6, p. 77]). In our case, we obtain a birational map to the curve

$$\tau^2 = \sigma[\sigma + 2n^2(m+n)^2][\sigma + 2m^2(m-n)^2] \tag{4}$$

given by

$$\frac{2}{(m^2-n^2)^2}\sigma = \alpha + R^2 - 2\left(\frac{m^2-2mn-n^2}{m^2-n^2}\right)R - 1$$
$$\tau = (m^2-n^2)[\sigma + 4m^2n^2]R - (m^2-2mn-n^2)\sigma.$$

Accordingly we can find a birational map from the original equation (3) to the elliptic curve (4), namely

$$\sigma = 2mn(m^2-n^2)\frac{ru}{sv}$$
$$\tau = 2mn(m^2-n^2)[(m^2-n^2)(r-s)u + 2mn(u+v)s]\frac{r}{s^2v} \tag{5}$$

with inverse

$$(m^2-n^2)\frac{r}{s}=\frac{\tau+(m^2-2mn-n^2)\sigma}{\sigma+4m^2n^2}$$
$$2mn\,\frac{u}{v}=\frac{\sigma[\sigma+4m^2n^2]}{\tau+(m^2-2mn-n^2)\sigma}. \tag{6}$$

At this stage it is more convenient to consider the curve (4) in the form

$$E'\colon \tau^2=\sigma[\sigma+2(\lambda+1)^2][\sigma+2\lambda^2(\lambda-1)^2], \tag{7}$$

where $\lambda=m/n$ and (σ, τ) have been replaced by $(\sigma n^4, \tau n^6)$.

There is a rational 2-isogeny υ from (7) to the curve

$$E\colon T^2=S[S-2(\lambda^2+1)^2][S-2(\lambda^2-2\lambda-1)^2] \tag{7'}$$

given by

$$\upsilon(\sigma,\tau)=(S,T)=\left(\frac{\tau^2}{\sigma^2},\left[1-\frac{4\lambda^2(\lambda^2-1)^2}{\sigma^2}\right]\tau\right). \tag{8}$$

The corresponding isogeny $\upsilon'\colon E\to E'$, satisfying $\upsilon\upsilon'$ being multiplication by 2 on E, is given by

$$\upsilon'(S,T)=(\sigma,\tau)=\left(\frac{T^2}{4S^2},\frac{1}{8}\left[1-\frac{4(\lambda^2+1)^2(\lambda^2-2\lambda-1)^2}{S^2}\right]T\right). \tag{8'}$$

We shall show that (7'), and hence (7), as an elliptic curve over the field $k=\mathbf{Q}(\lambda)$, has precisely one as the rank of its Mordell–Weil group of points defined over k. The presence of a rational 2-isogeny greatly simplifies the calculation of the rank, and the reader is referred to Birch and Swinnerton-Dyer [1] for details. In the language of Cassels [2], let G_υ (respectively $G_{\upsilon'}$) denote the group of υ-covers of E (υ'-covers of E') for which the corresponding curve is everywhere locally solvable over completions of k; and let G_υ^* (respectively $G_{\upsilon'}^*$) denote the subgroup of covers which actually posses a k-rational point. Then if g denotes the k-rational rank of E, a simple group theoretic argument shows that

$$2^{g+2}=[G_\upsilon^*][G_{\upsilon'}^*], \tag{9}$$

where square brackets denote the order of the particular group.

Now in any given instance it is straightforward to compute the groups G_υ and $G_{\upsilon'}$. The principal difficulty is deciding for those covers that are everywhere locally solvable whether they do indeed possess a globally

defined point. There is at present no known effective decision procedure for determining this.

In the case at hand, however, the computations can be carried out as follows.

The curves corresponding to the v-covers of E are those obtained in the classical manner, namely in (7′) put

$$S = \Delta A^2/B^2, \qquad \Delta,\ A,\ B \in \mathbf{Z}[\lambda],\ \Delta \text{ squarefree},\ (A, B) = 1. \tag{10}$$

This gives

$$(\Delta A^2 - 2(\lambda^2+1)^2 B^2)(\Delta A^2 - 2(\lambda^2 - 2\lambda - 1)^2 B^2) = \Delta C^2. \tag{11}$$

There is a one-to-one correspondence between the curves (11) and the elements of the group of v-covers of E. It is clearly necessary for local solvability of (11) that Δ divide $4(\lambda^2+1)^2\ (\lambda^2 - 2\lambda^2 - 1)^2$ and moreover, from (11), that the leading coefficient of Δ be positive.

Suppose first that $(\lambda^2+1) \mid \Delta$; then $(\lambda^2+1)^2 \nmid \Delta$. If $(\lambda^2+1) \mid A$, then (11) implies in turn $(\lambda^2+1) \mid C$, $(\lambda^2+1)^3 \mid (\Delta A^2 - 2(\lambda^2+1)^2 B^2)$, $(\lambda^2+1) \mid B$, a contradiction. So $(\lambda^2+1) \nmid A$, and similarly $(\lambda^2+1) \nmid B$.

But then modulo $(\lambda^2+1)^2$, (11) gives

$$-2\Delta(\lambda^2 - 2\lambda - 1)^2 A^2 B^2 \equiv \Delta C^2$$

hence

$$-2 \equiv \text{square} \qquad \bmod(\lambda^2+1). \tag{12}$$

However, (12) forces -2 to be a square in $Z[i]$, which is a contradiction. Thus $(\lambda^2+1)^2 \nmid \Delta$.

Suppose second that $(\lambda^2 - 2\lambda - 1) \mid \Delta$. As above, $(\lambda^2 - 2\lambda - 1) \nmid AB$, yet

$$-2(\lambda^2+1)^2 A^2 B^2 \equiv \text{square} \qquad \bmod(\lambda^2 - 2\lambda - 1),$$

giving

$$-2 \equiv \text{square} \qquad \bmod(\lambda^2 - 2\lambda - 1).$$

This forces -2 to be a square in $Z[\sqrt{2}]$, a contradiction. So $(\lambda^2 - 2\lambda - 1) \nmid \Delta$.

There are thus only two possibilities for Δ, namely $\Delta = 1, 2$, corresponding to curves (11) with global points, viz.,

Δ	(A, B)
1	$(1, 0)$
2	$(\lambda^2+1, 1)$

(13)

At (9), therefore, we have $[G_v^*] = 2$.

We perform a similar calculation for the curve E' at (7) in order to determine $[G_v^*]$.

Put

$$\sigma = \delta a^2/b^2, \qquad \delta,\ a,\ b \in \mathbf{Z}[\lambda],\ \delta \text{ squarefree},\ (a, b) = 1. \tag{14}$$

This gives

$$(\delta a^2 + 2(\lambda+1)^2 b^2)(\delta a^2 + 2\lambda^2(\lambda-1)^2 b^2) = \delta c^2, \tag{15}$$

where, for local solvability, it is necessary that δ divide $4\lambda^2(\lambda-1)^2(\lambda+1)^2$.

Suppose $\lambda \mid \delta$. As above, $\lambda \nmid ab$. Then (15) implies

$$2\delta a^2 b^2 \equiv \delta c^2 \qquad \mod \lambda^2$$

so that

$$2 \equiv \text{square} \qquad \mod \lambda,$$

which is impossible. Thus $\lambda \nmid \delta$. Mutatis mutandis, $(\lambda-1) \nmid \delta$, $(\lambda+1) \nmid \delta$. There are thus precisely four remaining possibilities for δ, namely $\delta = \pm 1$, ± 2, corresponding to curves (15) with global points, viz.,

δ	(a, b)
1	$(1, 0)$
-1	$(2\lambda, 1)$
2	$(\lambda(\lambda+1), 1)$
-2	$(\lambda(\lambda-1), 1)$

(16)

Consequently $[G_v^*] = 2^2$ and from (9), the rank of E and of E' is thus equal to 1.

It is now possible to verify that the following point is a generator for the k-rational Mordell–Weil group of E',

$$(2(\lambda-1)^2,\ 4(\lambda-1)^2(\lambda^2+1)), \tag{17}$$

corresponding to the generator at (4) given by

$$P = (2n^2(m-n)^2,\ 4n^2(m-n)^2(m^2+n^2)). \tag{18}$$

The details are modelled on the example of Cassels, Ellison, and Pfister [3], but are sufficiently tiresome that we omit them.

The generator P at (18) pulls back via the maps (6) to the point of (3) given by

$$\frac{r}{s} = \frac{m-n}{m+n}, \qquad \frac{u}{v} = \frac{n}{m}, \tag{19}$$

corresponding to the solution of (1)

$$(X, Y) = \left(-\frac{1}{M}, -M\right).$$

Since the rank of E' is one, and the only points on E' of finite order are those of order 2, then any k-rational point of E' is of type $\mu P + P_0$, $\mu \in Z$, P_0 a point of order 2. It is readily verified that if μP corresponds via the maps (6) to the values (r, s, u, v), then $\mu P + (0, 0)$ corresponds to the values $(-s, r, -v, u)$: and so both points lead to the same values of (X, Y) at (1).

Now let P_0 denote the point of order 2

$$(-2n^2(m+n)^2, 0).$$

The result of adding P_0 is characterized by the following lemma.

LEMMA. *Let* $\mu \in Z$.

(i) *If* $2\mu P + P_0$ *corresponds to the values* (r, s, u, v), *then* $(2\mu + 1)P$ *corresponds to* $(-s, r, u, v)$;

(ii) *If* $(2\mu + 1)P + P_0$ *corresponds to the values* (r, s, u, v), *then* $-2\mu P$ *corresponds to* $(-s, r, u, v)$.

Proof. Formula chasing using the addition law on the elliptic curve.

As a corollary to the lemma, it follows that to find all solutions (X, Y) of the original equation (1), it suffices only to investigate the pullbacks of the integer multiples μP on E'. We can even reduce to considering only the positive multiples of P, by introducing the process of inversion. We refer the reader to Guy [5] for a detailed description of a family of eight solutions of (1) associated with any given solution (but only two of this family of eight, a solution and its inversion, having the same slope).

In formulae, the inversion of (X, Y) is the solution

$$\left(\frac{1 - X - Y + X^2}{1 - XY}, \frac{1 - X - Y + Y^2}{1 - XY}\right).$$

The required result is as follows, again proved by formula chasing.

LEMMA. *Denote by* (X_n, Y_n) *the solution of* (1) *obtained from the point* nP *on* E'. *Then the solution* $(X_{-\mu}, Y_{-\mu})$ *is the inversion of the solution* $(X_{\mu+1}, Y_{\mu+1})$.

Accordingly, to find all the k-rational points of (3), it is only necessary to investigate the integer multiples μP on E', with $\mu > 0$.

By calculation we have

$$2P = (\tfrac{1}{4}(m^2+2mn-n^2)^2,$$
$$-\tfrac{1}{8}(m^2+2mn-n^2)(m^2+2mn+3n^2)(3m^2-2mn+n^2))$$

with pullback

$$\frac{r}{s} = -\frac{(m^2+2mn-n^2)}{2(m^2-n^2)}$$
$$\frac{u}{v} = -\frac{(m^2+2mn-n^2)}{4mn}. \tag{20}$$

Denote now the pullback of μP by $(r_\mu, s_\mu, u_\mu, v_\mu)$. Then the group law on (3) amounts to the following, on putting

$$S = s_\mu / r_\mu, \qquad V = v_\mu / u_\mu \qquad (\mu \geqslant 2):$$

$$r_{\mu+1} : s_{\mu+1};\ u_{\mu+1} : v_{\mu+1}$$
$$= (m-nV)\left[\left(\frac{m^4-n^4}{mn}\right)SV - (m^2+2mn+3n^2)V^2\right.$$
$$\left. + 2\frac{n}{m}(m^2-2mn-n^2)V - (m^2+2mn-n^2)\right]:$$
$$(n+mV)\left[2(m^2+n^2)SV - \frac{n(m+n)}{m(m-n)}(3m^2-2mn+n^2)V^2\right.$$
$$\left. + 2\left(\frac{m+n}{m-n}\right)(m^2-2mn-n^2)V - \frac{m(m+n)}{n(m-n)}(m^2-2mn-n^2)\right];$$
$$((m+n)-(m-n)S)\left[4\frac{mn(m^2+n^2)}{m^2-n^2}SV - (3m^2-2mn+n^2)S^2\right.$$
$$\left. - 2\left(\frac{m-n}{m+n}\right)(m^2-2mn-n^2)S + (m^2-2mn-n^2)\right]:$$
$$((m-n)+(m+n)S)\left[2(m^2+n^2)SV - \frac{m(m-n)}{n(m+n)}(m^2+2mn+3n^2)S^2\right.$$
$$\left. - 2\frac{m}{n}(m^2-2mn-n^2)S + \frac{m(m+n)}{n(m-n)}(m^2-2mn-n^2)\right].$$

These recursion formulae now mean it is possible to compute directly the solutions $(r_\mu, s_\mu, u_\mu, v_\mu)$ starting with the values for $\mu = 2$ at (20). But the solutions have rapidly increasing degree. We have, for instance,

$$
\begin{aligned}
&(r_3 : s_3 ; u_3 : v_3) \\
&\quad = (m-n)(m^2+2mn+3n^2)(7m^4+12m^3n+6m^2n^2+4mn^3-n^4): \\
&\qquad (m+n)(3m^2-2mn+n^2)(m^4+4m^3n-6m^2n^2+12mn^3-7n^4); \\
&\qquad n(3m^2-2mn+n^2)(7m^4+12m^3n+6m^2n^2+4mn^3-n^4): \\
&\qquad m(m^2+2mn+3n^2)(m^4+4m^3n-6m^2n^2+12mn^3-7n^4).
\end{aligned}
$$

The inversion of this solution is just

$$
\begin{aligned}
(r_{-2} : s_{-2} ; u_{-2} : v_{-2}) = {} & (m^2+2mn-n^2)(5m^4+4m^3n-6m^2n^2-4mn^3+5n^4): \\
& 2(m^2-n^2)(m^4+4m^3n+18m^2n^2-4mn^3+n^4); \\
& (m^2+2mn-n^2)(m^4+4m^3n+18m^2n^2-4mn^3+n^4): \\
& 4mn(5m^4+4m^3n-6m^2n^2-4mn^3+5n^4).
\end{aligned}
$$

In this manner, we can construct an infinity of parametrized solutions to the Δ-problem. The first couple of solutions are as follows. The point P, using (19) and (2), gives the solution

$$X = \frac{2mn}{n^2-m^2}, \qquad Y = \frac{n^2-m^2}{2mn};$$

the point $2P$, using (20) and (2), gives the solution

$$
\begin{aligned}
X &= \frac{(m^2-2mn-n^2)(3m^2+2mn-3n^2)}{4(m^2-n^2)(m^2+2mn-n^2)}, \\
Y &= \frac{(m^2-2mn-n^2)(m^2+6mn-n^2)}{-8mn(m^2+2mn-n^2)}.
\end{aligned}
$$

The reader may construct further examples using the recursion developed above, together with the maps (2). It is of interest to remark that neither of the above solutions for any value of m and n corresponds geometrically to a configuration in which the point (X, Y) lies inside the unit square.

The first solution translates into a degenerate lambda-configuration, the second into a non-degenerate lambda-configuration. The further restriction that this lambda-configuration extend to a rational chi-configuration (cf. Figs. 3 and 5) is that

$$(MX)^2 + Y^2 = \text{square},$$

which simplifies to the condition

$$(3m^2+2mn-3n^2)^2 + (m^2+6mn-n^2)^2 = \text{square},$$

i.e.,

$$2(5m^4 + 12m^3n + 10m^2n^2 - 12nm^3 + 5n^4) = \text{square}.$$

This forces $m \equiv n \equiv 1 \bmod 2$, giving $8 \equiv$ square mod 16, an impossibility. Consequently, no rational chi-configurations arise from the above parametrizations.

All these parametrized solutions of course correspond to a slope of $(m^2 - n^2)/2mn$; and so for a given numerical rectangular number M, there will similarly correspond an infinity of numerical solutions. If, in the specialization of m, n to integer values, the rank of the specialized curve E' (now over Q) is still equal to one, then provided the generator at (18) remains a generator under specialization, we will have determined all the rational solutions for the numerical slope $(m^2 - n^2)/2mn$. In practice, the rank of the specialized curve E' can quite often exceed one, and we investigate these numerical instances in the next section.

4

We turn now to numerical solutions of (3) for prescribed rational values of m/n, where we adopt the convention that $(m, n) = 1$ and $m + n \equiv 1 \bmod 2$.

The v-covers of E are still given by equations of type (11), which we write as

$$(\Delta A^2 - 2(m^2 + n^2)^2 B^2)(\Delta A^2 - 2(m^2 - 2mn - n^2)^2 B^2) = \Delta C^2. \qquad (21)$$

LEMMA 1. *If* (21) *has a non-trivial solution, then* $\Delta > 0$.

Proof. Obvious.

LEMMA 2. *Suppose* P *is a prime number,* $P \equiv +1 \bmod 8$ *and* $P \mid mn(m^2 - n^2)$. *Suppose further* $(\Delta/P) = -1$. *Then* (21) *has no non-trivial solutions.*

Proof. Rewrite (21) in the form

$$(\Delta A^2 - 2(m^4 - 2m^3n + 2m^2n^2 + 2mn^3 + n^4) B^2)^2 - 16m^2n^2(m^2 - n^2)^2 B^4 = \Delta C^2,$$

where, for a non-trivial solution, we have $(A, B) = 1$. Since $P \mid mn(m^2 - n^2)$ and $(\Delta/P) = -1$, then

$$\Delta A^2 - 2(m^4 - 2m^3n + 2m^2n^2 + 2mn^3 + n^4) B^2 \equiv C \equiv 0 \qquad \bmod P.$$

Thus

$$\Delta A^2 - 2(m^2+n^2)^2 B^2 \equiv 0 \qquad \text{mod } P.$$

But $(2/P) = +1$, $(\Delta/P) = -1$, giving $A \equiv B \equiv 0 \bmod P$, a contradiction.

In similar fashion we have that v'-covers of E' are given by equations of type (15), which we write as

$$(\delta a^2 + 2m^2(m-n)^2 b^2)(\delta a^2 + 2n^2(m+n)^2 b^2) = \delta c^2. \tag{22}$$

LEMMA 3. *Suppose p is a prime, $p \equiv 1 \bmod 8$, and $p \mid (m^2+n^2)(m^2-2mn-n^2)$. Suppose further $(\delta/p) = -1$. Then (22) has no non-trivial solution.*

Proof. Rewrite (22) in the form

$$(\delta a^2 + (m^4 - 2m^3n + 2m^2n^2 + 2mn^3 + n^4)b^2)^2 - (m^2+n^2)^2 (m^2-2mn-n^2)^2 b^4 = \delta c^2,$$

where, for a non-trivial solution, $(a, b) = 1$.

Since $m^4 - 2m^3n - 2mn^3 + n^4 \equiv (m^2+n^2)(m^2-2mn-n^2) \equiv 0 \bmod p$, then $(\delta/p) = -1$ implies

$$\delta a^2 + 2n^2(m+n)^2 b^2 \equiv c \equiv 0 \qquad \text{mod } p.$$

But $(-2/p) = +1$, $(\delta/p) = -1$, and $p \mid n(m+n)$. Thus $a \equiv b \equiv 0 \bmod p$, a contradiction.

LEMMA 4. *If (21) has a non-trivial solution, and P is an odd prime dividing Δ, then $P \equiv 1 \bmod 8$.*

Proof. Certainly, from (21) we have Δ(squarefree) divides $2(m^2+n^2)(m^2-2mn-n^2)$, so that necessarily Δ is of shape $\alpha\beta$ or $2\alpha\beta$, where α, β are odd, $(\alpha, \beta) = 1$, and $\alpha \mid m^2+n^2$, $\beta \mid m^2-2mn-n^2$.

Consider first $\Delta = \alpha\beta$. Then

$$\left(\beta A^2 - \frac{2(m^2+n^2)^2}{\alpha} B^2\right)\left(\alpha A^2 - \frac{2(m^2-2mn-n^2)^2}{\beta} B^2\right) = C^2. \tag{23}$$

Suppose $\alpha \neq \pm 1$, and let P be a prime divisor of α. Then (23) implies $ABC \not\equiv 0 \bmod P$, yet

$$-2(m^2-2mn-n^2)^2 A^2 B^2 \equiv C^2 \qquad \text{mod } P$$

which forces $(-2/P) = +1$, i.e., $P \equiv 1, 3 \bmod 8$. However, $P \mid m^2+n^2$, so $P \equiv 1 \bmod 4$. Thus $P \equiv 1 \bmod 8$.

Suppose $\beta \neq \pm 1$, and let P divide β. As above,

$$-2(m^2+n^2)\,A^2B^2 \equiv C^2 \qquad \bmod P$$
$$ABC \not\equiv 0 \qquad \bmod P,$$

so that $(-2/P) = +1$ and $P \equiv 1,\ 3 \bmod 8$. However, $P \mid m^2 - 2mn - n^2$ implies $(2/P) = +1$, so that $P \equiv 1,\ 7 \bmod 8$. Thus $P \equiv 1 \bmod 8$. Similar arguments apply to the case $\Delta = 2\alpha\beta$, and the result of the lemma follows.

LEMMA 5. *If* (22) *has a non-trivial solution, and* p *is an odd prime dividing* δ, *then* $p \equiv \pm 1 \bmod 8$.

Proof. As above, δ (squarefree) divides $2mn(m^2-n^2)$, so we can write $\delta = \alpha\beta$ or $2\alpha\beta$ where α, β are odd, $\alpha \mid m(m-n)$, $\beta \mid n(m+n)$, and $(\alpha, \beta) = 1$. If $\delta = \alpha\beta$, then

$$\left(\beta a^2 + \frac{2m^2(m-n)^2}{\alpha}\, b^2\right)\left(\alpha a^2 + \frac{2n^2(m+n)^2}{\beta}\, b^2\right) = c^2. \tag{24}$$

Let p be a prime divisor of α. Then from (24), $abc \not\equiv 0 \bmod p$, yet

$$2n^2(m+n)^2\,a^2b^2 \equiv c^2 \qquad \bmod p$$

which forces $(2/p) = +1$. Similarly if p divides β, then

$$2m^2(m-n)^2\,a^2b^2 \equiv c^2 \qquad \bmod p,$$

again forcing $(2/p) = +1$.

The same conclusion holds for $\delta = 2\alpha\beta$, and the lemma follows.

THEOREM 6. *Let there be* j *prime divisors* p_1 *of* $(m^2+n^2)(m^2-2mn-n^2)$ *which satisfy* $p_1 \equiv 1 \bmod 8$. *Let there be* k *prime divisors* p_2 *of* $mn(m^2-n^2)$ *which satisfy* $p_2 \equiv \pm 1 \bmod 8$.

Then the rank g *of* (4), *and hence* (3), *satisfies*

$$1 \leqslant g \leqslant j + k + 1.$$

Proof. That $g \geqslant 1$ follows from (13) and (16), since these imply $2 \mid [G_v^*]$ and $4 \mid [G_{v'}^*]$, respectively.

On the other hand, the order of $[G_v^*]$, in virtue of the previous lemmas, is at most 2^{j+1}; and the order of $[G_{v'}^*]$ is at most 2^{k+2} (recall that δ may be negative). The upper bound thus follows from (9).

Table I shows our numerical results for pairs m, n satisfying $2 \leqslant m \leqslant 16$, $3 \leqslant m+n \leqslant 17$, $m \equiv 0 \bmod 2$, $n \equiv 1 \bmod 2$, $(m, n) = 1$. The values of m, n occur in the first two columns. The succeeding six columns give the

TABLE I

m	n	m^2+n^2	$m^2-2mn-n^2$	m	n	$m+n$	$m-n$		Rank
2	1	5	—	—	—	3	—	—	1
2	−1	5	7	—	—	—	3	—	1
4	1	**17**	7	—	—	5	3	$\Delta = 17$: (2; 1; 30)	2
4	−1	**17**	23	—	—	3	5	$\Delta = 17$: (8; 1; 30)	2
2	3	13	**17**	—	3	5	—	$\Delta = 17$: (2; 1; 90)	2
2	−3	13	7	—	3	—	5	—	1
6	1	37	23	3	—	**7**	5	$\delta = 7$: (3; 1; 207)	2
6	−1	37	47	3	—	5	7	$\delta = 7$: (5; 1; 345)	2
4	3	5	**17**	—	3	**7**	—	—	1
4	−3	5	31	—	3	—	**7**	$\delta = 7$: (1; 1; 75)	2
2	5	29	**41**	—	5	**7**	3	—	1
2	−5	29	—	—	5	3	**7**	$\delta = 7$: (5; 1; 225)	2
8	1	5, 13	47	—	—	3	**7**	$\delta = 7$: (27; 1; 2925)	2
8	−1	5, 13	79	—	—	**7**	3	$\delta = 7$: (304; 1; 246480)	2
4	5	**41**	7	—	5	3	—	$\Delta = 41$: (1; 1; 621)	2
4	−5	**41**	31	—	5	—	3	$\Delta = 41$: (10; 1; 198)	2
2	7	53	**73**	—	**7**	3	5		1
2	−7	53	**17**	—	**7**	5	3	—	1
10	1	101	79	5	—	11	3	—	1
10	−1	101	7, **17**	5	—	3	11	$\Delta = 17$: (26; 1; 2970)	2
8	3	**73**	7	—	3	11	5	$\Delta = 73$: (16; 1; 1430)	2
8	−3	**73**	103	—	3	5	11	$\Delta = 73$: (6; 1; 1430)	2
6	5	61	7	3	5	11	–	—	1
6	−5	61	71	3	5	—	11	—	1
4	7	5, 13	**89**	—	**7**	11	3	—	1
4	−7	5, 13	23	—	**7**	3	11	$\delta = 7$: (37; 1; 4485)	2
2	9	5, **17**	**113**	—	3	11	**7**	$\Delta = 113$: (10; 1; 630)	2
2	−9	5, **17**	41	—	3	**7**	11	$\Delta = 17.41$: (2; 1; 98)	2
12	1	5, 29	7, **17**	3	—	13	11	$\Delta = 17$: (29; 1; 4785)	2
12	−1	5, 29	167	3	—	11	13	—	1
10	3	109	31	5	3	13	**7**	$\delta = 7$: (180; 1; 88140)	2

10	−3	109	151	5	3	**7**	13	$\delta = 7$: (5; 1; 2265)	2
8	5	**89**	**41**	—	5	13	3		$1 \leqslant \leqslant 3$
8	−5	**89**	7, **17**	—	5	3	13		$1 \leqslant \leqslant 3$
6	7	5, **17**	**97**	3	**7**	13	—	$\Delta = 17.97$: (4; 1; 234)	2
6	−7	5, **17**	71	3	**7**	—	13	—	1
4	9	**97**	**137**	—	3	13	5		$1 \leqslant \leqslant 2$
4	−9	**97**	7	—	3	5	13	$\Delta = 97$: (154; 3; 224770)	2
2	11	5	7, 23	—	11	13	3	—	1
2	−11	5	**73**	—	11	3	13	$\Delta = 73$: (61; 1; 29315)	2
14	1	197	167	**7**	—	3, 5	13	$\delta = 7$: (1405; 31; 12559425)	2
14	−1	197	223	**7**	—	13	3, 5	$\delta = 7$: (13; 1; 4407)	2
8	7	**113**	**97**	—	**7**	3, 5	—	$\Delta = 113$: (4; 1; 1890)	2
8	−7	**113**	127	—	**7**	—	3, 5		$1 \leqslant \leqslant 3$
4	11	**137**	**193**	—	11	3, 5	**7**	$\delta = 7$: (24; 1; 6840)	$2 \leqslant \leqslant 4$
4	−11	**137**	**17**	—	11	**7**	3, 5	$\Delta = 137$: (2; 1; 90)	2
2	13	173	7, 31	—	13	3, 5	11	—	1
2	−13	173	**113**	—	13	11	3, 5	$\Delta = 113$: (31; 1; 5985)	2
16	1	**257**	223	—	—	**17**	3, 5		$1 \leqslant \leqslant 3$
16	−1	**257**	7, **41**	—	—	3, 5	**17**	$\Delta = 257$: (28; 1; 3150)	2
14	3	5, **41**	103	7	3	**17**	11	$\delta = 7.17$: (3; 1; 1599)	2
14	−3	5, **41**	271	7	3	11	**17**	$\delta = 7.17$: (3; 1; 1767)	2
12	5	13	—	3	5	**17**	**7**	—	1
12	−5	13	239	3	5	**7**	**17**	—	1
10	7	149	**89**	5	7	**17**	3	$\delta = 17$: (56; 1; 16268)	2
10	−7	149	191	5	7	3	**17**	—	1
8	9	5, 29	7, 23	—	3	**17**	—	$\delta = 17$: (416; 19; 1867600)	2
8	−9	5, 29	127	—	3	—	**17**	$\delta = 17$: (128; 1; 71920)	2
6	11	157	7, 31	3	11	**17**	5	$\delta = 17$: (627; 8; 2112495)	2
6	−11	157	47	3	11	5	**17**	$\delta = 17$: (24; 1; 5340)	2
4	13	5, 37	**257**	—	13	**17**	3		$1 \leqslant \leqslant 3$
4	−13	5, 37	7	—	13	3	**17**	$\delta = 17$: (83; 2; 45325)	2
2	15	229	**281**	—	3, 5	**17**	13	$\Delta = 281$: (35; 1; 12597) $\delta = 17$: (80; 1; 39340)	3
2	−15	229	7, 23	—	3, 5	13	17	$\delta = 17$: (845; 8; 3505775)	2

odd prime factors of m^2+n^2, $m^2-2mn-n^2$, m, n, $m+n$, and $m-n$, respectively. Potential odd prime factors of δ and Δ, corresponding to Lemmas 2–5 appear in boldface type.

The penultimate column contains the values of Δ and δ, if any, for which there is a global point on the corresponding covers (21) and (22): the global point (A, B, C) or (a, b, c), respectively, is given.

The final column contains the rank if there is now sufficient information for it to be computed explicitly. In the case that there exist values of Δ and δ for which we have not determined whether the corresponding covers are globally solvable, then bounds on the rank are given using the available information. In actual fact, for four entries in Table I, some additional calculations were necessary to eliminate certain possibilities for δ, Δ. These are the instances $(m, n)=(4, 9)$ with $\Delta=97$ and $(m, n)=(10, -7)$, $(12, 5)$, $(12, -5)$ with in each case $\delta=7$, 17, and 7.17. The arguments for elimination are based on straightforward congruences and present no difficulty. They may safely be left as exercises for the interested reader.

Remark. If we consider the parametrized family of curves (3) for which

$$(m, n)=(2\alpha(\alpha-1), 2\alpha+1)$$

then the rational $Q(\alpha)$-rank is equal to 2. This is proved as in Section 3.

Finally, Table II shows our calculations of particular values of X, Y corresponding to the slope $(m^2-n^2)/2mn$. Of course, in every instance there is the basic solution given by $X=1/Y=2mn/(n^2-m^2)$. In the case that the rank of the corresponding curve equals 1, then there is but a single infinity of solutions (X, Y) and it is likely in the numerical instances we are considering (although we have not checked specifically) that the above solution corresponds to a generator. In this case, all solutions can be found by means of the recursion formulae developed in Section 3. We thus only present solutions for the curves with rank at least 2. Those we do provide are obtained by pulling back the points indicated in column 9 of the first table. In some cases, rather large numbers resulted, and so we actually considered, for a given point (σ, τ) on the curve E', the four solutions (of same slope) resulting from the pullbacks of the two points (σ, τ) and $(\sigma, \tau)+P_0$, together with the corresponding inversion of these two solutions. Table II lists the simplest of these four solutions.

As an example, consider the instance $(m, n)=(2, 15)$ (which is our only specific example where the rank is 3).

The curve (4), together with its 2-isogenous curve, has equations

$$\tau^2=\sigma(\sigma+130050)(\sigma+1352), \tag{25}$$

$$T^2=S(S-104882)(S-157922); \tag{26}$$

TABLE II

m	n	X	Y
4	1	28/45	7/24
4	−1	−472/3465	5785/1848
2	3	221/60	−17/144
6	1	21/20	55/48
6	−1	279/440	2183/1056
4	−3	4/3	65/72
2	−5	−5/12	−39/80
8	1	28/45	−39/80
8	−1	52/675	5561/1200
4	5	225620/67221	140361/298760
4	−5	−65260/247779	788201/1101240
10	−1	334291/386100	129809/78000
8	3	3426032/2629935	3091313/2295216
8	−3	169692/71995	−34865/62842
4	−7	−20/99	7/24
2	9	435/308	17/144
2	−9	1664/3927	−427/1836
12	1	2349/2860	−31/480
10	3	−15965/6708	−127751/30960
10	−3	165/52	−551/240
6	7	−396/403	3403/2604
4	−9	−6047157228/19762625285	−3918874505/21890908008
2	−11	−88394117629/154741721940	−184942371489/58193468080
14	1	92031347251/104412310860	373081905/2141790992
14	−1	451/780	63/16
8	7	−3848/1335	4785/9968
4	11	91/60	135/352
4	−11	−5332/1995	−5655/1672
2	−13	16662822019/33446023380	−6242636417/10540564944
16	−1	198008/173145	−3135/21728
14	3	24/143	−133/156
14	−3	−689/1320	6319/1440
10	7	595/468	23999/21840
8	9	348/3355	534239/483120
8	−9	−480/31	−4223/4464
6	11	−46609/59280	3365105/1564992
6	−11	−549/1820	7775/48048
4	−13	28/45	231/520
2	15	44936499/66428180	39526481/18034800
2	15	25/312	6319/1440
2	−15	25425/18928	197809/87360

and from the appropriate row of the first table, we have that (25) and (26) contain the respective points

$$(\sigma, \tau) = (17.80^2, 17.80.39340), \tag{27}$$

$$(S, T) = (281.35^2, 281.35.12597). \tag{28}$$

The maps (6) only allow a pullback of points on (25). But we can use the maps (8′) first to map the point (28) to the following point of (25):

$$(\sigma', \tau') = \left(\frac{12597^2}{70^2}, \frac{12597.281.1290861}{70^3}\right). \tag{29}$$

It is now simply a matter of computing for the points (27) and (29) the associated values of r, s, u, v, using (6), and then the final values of X, Y, using (2).

Here, we have for (27) that

$$\frac{r}{s} = -\frac{12}{13}, \qquad \frac{u}{v} = \frac{80}{9}$$

and for (29),

$$\frac{r}{s} = \frac{-4199}{7910}, \qquad \frac{u}{v} = \frac{6441}{1400}.$$

These in turn give the respective solutions for (X, Y):

$$(X, Y) = \left(\frac{25}{312}, \frac{6319}{1440}\right); \qquad (X, Y) = \left(\frac{44{,}936{,}499}{66{,}428{,}180}, \frac{39{,}526{,}481}{18{,}034{,}800}\right). \tag{30}$$

The inverse solutions to (30) involve much larger numbers, similarly for the pullbacks (and their inversions) of the points at (27) and (29) added to P_0. Consequently, the solutions listed in Table II are those at (30).

REFERENCES

1. B. J. BIRCH AND H. P. F. SWINNERTON-DYER, Notes on elliptic curves II, *J. Reine Angew. Math.* **218** (1965), 79–108.
2. J. W. S. CASSELS, Diophantine equations with special reference to elliptic curves, *J. London Math. Soc.* **41** (1966), 193–291.
3. J. W. S. CASSELS, W. J. ELLISON, AND A. PFISTER, On sums of squares and on elliptic curves over function fields, *J. Number Theory* **3** (1971), 125–149.
4. R. K. GUY, Tiling the square with rational triangles, "Proc. NATO ASI, Banff, 1988," Kluwer, Dordrecht (1989), 45–101.
5. R. K. GUY, The eight-lambdas configuration arising from some Pythagorean Diophantine equations, *in* "Proc. Conf. Discrete Geom., Salzburg, 1985."
6. L. J. MORDELL, "Diophantine Equations," Academic Press, New York, 1969.